

Cite as 2023 Ark. App. 295
ARKANSAS COURT OF APPEALS

DIVISION III
No. CR-22-572

JONATHAN WALKER

APPELLANT

V.

STATE OF ARKANSAS

APPELLEE

Opinion Delivered May 17, 2023

APPEAL FROM THE CLARK
COUNTY CIRCUIT COURT
[NO. 10CR-20-107]

HONORABLE BLAKE BATSON, JUDGE

AFFIRMED AS MODIFIED

KENNETH S. HIXSON, Judge

Appellant Jonathan Walker was convicted in a jury trial of thirty counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child and Walker was sentenced as a habitual offender to thirty consecutive fifteen-year prison terms. Pursuant to Ark. Code Ann. § 5-27-602(a)(2) (Repl. 2013), a person commits this offense “if the person knowingly possesses or views through any means, including on the Internet, any photograph, film, videotape, computer program or file . . . or any other reproduction that depicts a child or incorporates the image of a child engaging in sexually explicit conduct.”¹ Walker’s convictions arose from a cyber tip from an internet-service provider that resulted in a police search of Walker’s computer equipment on which they

¹A “Child” means any person under seventeen years of age.” Ark. Code Ann. § 5-27-601(1) (Repl. 2013).

found images of juvenile males in sexually explicit poses and juvenile males engaged in sexually explicit conduct with adult males. On appeal, Walker does not challenge the sufficiency of the evidence supporting the convictions; rather, Walker raises these seven arguments: (1) the trial court erred in not recusing; (2) the trial court erred in admitting the items seized from his home because the search was illegal; (3) the trial court erred in admitting his prior convictions from Oregon during the guilt phase of the trial; (4) the trial court erred in admitting images from his computer for which he was not charged; (5) the trial court erred in allowing the State to play a portion of Walker's statement to the police wherein his sex-offender status was discussed; (6) the trial court erred in admitting Walker's Oregon "pen pack" during the guilt phase of the trial; and (7) the trial court erred in refusing Walker's affirmative-defense jury instruction that he reasonably believed five of the persons depicted in the images were seventeen years of age or older. We affirm Walker's convictions, and we modify the sentencing order as explained below.

I. *Facts*

On April 28, 2020, an image or file from Walker's computer was uploaded to a Microsoft OneDrive account. Microsoft's internal algorithm program² determined, based on the "hash value" of the file, that the image was a known catalogued image of child

²Neither the mechanics nor the accuracy of the Microsoft internal algorithm program was challenged at trial and neither is an issue in this appeal.

pornography.³ Without viewing the image and based solely on the hash value, Microsoft reported the image, the Internet Protocol (IP) address, and the date uploaded to the National Center for Missing and Exploited Children (NCMEC).⁴ The IP address was associated with Suddenlink Communications. NCMEC then forwarded this information, along with the image, to the Arkansas State Police.

The Arkansas State Police has an internal task force referred to as the Internet Crimes Against Children Task Force (ICAC). Special Agents Adam Pinner and Corwin Battle are assigned to the task force and investigated the cyber tip from NCMEC. Agent Pinner reviewed the image and determined it constituted child pornography. Through its investigation, the ICAC determined that the account name associated with the IP address was Jonathan Walker with a service and billing address at an apartment in Arkadelphia.

³In technical terms, a hash value is an “algorithmic calculation that yields an alphanumeric value for a file.” *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). More simply, a hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file’s contents. In the words of one commentator, “[t]he concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data.” Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005).

⁴NCMEC is a nonprofit private entity. NCMEC’s Cyber Tipline is the nation’s centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child-sexual-abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the Internet.

Agent Pinner swore out an affidavit for a search warrant for Walker's apartment and computer equipment. The affidavit set forth the facts constituting probable cause, which included information that the uploaded image was of a prepubescent male depicting nudity in a sexually suggestive pose. Based on the information in the affidavit, a search warrant was issued.⁵

During the search of Walker's apartment, the police seized several laptop computers, including a Dell computer with a Toshiba hard drive. While Walker's apartment was being searched, Walker was Mirandized and gave a statement. In his statement, Walker admitted that he lived alone at the apartment, that his wireless Internet was password protected, and that the computers belonged to him. Walker denied possessing any child pornography.

Agent Battle subsequently conducted a forensic examination of the Toshiba hard drive in the Dell computer seized from Walker's apartment. According to Agent Battle's trial testimony, the Windows operating system had the username "Jonathan." Agent Battle testified that the hard drive was divided into seven partitions and that the seventh partition of the hard drive contained hundreds of images and videos of child-sexual-abuse material, which he stated is synonymous with child pornography. The seventh partition also contained images of Walker, his car, and his marriage license. Agent Battle testified that

⁵As will be discussed, *infra*, Walker filed a motion to suppress on the grounds that the affidavit for search warrant lacked probable cause, and after a suppression hearing, Walker's motion was denied.

State's exhibits 1-30 contained images of child-sexual-abuse material retrieved from Walker's computers, and these exhibits were admitted into evidence at the jury trial.⁶

From this evidence, the jury found Walker guilty of thirty counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child, and the jury sentenced Walker to a total of 450 years in prison. Walker now appeals.

II. *Points on Appeal*

A. The Trial Judge's Refusal to Recuse Himself

Walker's first argument on appeal is that the trial judge abused his discretion in refusing to recuse himself. During a pretrial hearing, Walker's attorney raised the issue of Circuit Judge Blake Batson's former law partnership with the prosecutor, Dan Turner. At the pretrial hearing, Walker's counsel argued:

My client feels that he's being prejudiced about the fact that you and the prosecutor used to be in business together. And he believes that . . . representation of Arnold, Batson, Turner, and Turner is still showing up on the Internet, even if it's not on the sign.

Prosecutor Turner responded:

I think this court has dealt with this very issue numerous times over the last twenty months. I don't think that's a basis for a requirement that the court recuse.

Judge Batson declined to recuse himself and stated:

Mr. Walker, there are specific rules this court complies with. And the fact that there may be something on the Internet that indicates our past business relationship, it's not sufficient for disqualification.

⁶Several of the charged counts were video files, and in support of these counts, the State offered screen shots from the videos rather than the videos themselves.

Walker now assigns error to the trial judge's refusal to recuse himself due to the trial judge's former partnership with Turner and the alleged appearance of impropriety.

Canon 2.11(A)(1) of the Arkansas Code of Judicial Conduct states that “[a] judge shall disqualify himself or herself in any proceeding in which the judge’s impartiality might be reasonably questioned, including . . .” when “[t]he judge has a personal bias or prejudice concerning a party or a party’s lawyer[.]” Walker argues that because there was still information online that the trial judge and the prosecutor were practicing law together twenty months after the judge took the bench, the trial judge’s impartiality was reasonably questioned, and there was at least an appearance of impropriety. Walker cites *Burrows v. Forrest City*, 260 Ark. 712, 543 S.W.2d 488 (1976), for the proposition that a trial judge should not remain on a case where there exists even an appearance of impropriety.⁷ Walker further asserts that the trial judge’s adverse rulings indicated bias or an appearance of bias. For these reasons, Walker contends that the trial judge’s refusal to recuse himself constituted reversible error. We disagree.

In *Owens v. State*, 354 Ark. 644, 654-55, 128 S.W.3d 445, 451-52 (2003), the supreme court set forth these standards:

A trial judge has a duty not to recuse from a case where no prejudice exists. Thus, if there is no valid reason for the judge to disqualify himself or herself, he or she has a duty to remain on a case. There is a presumption that judges are impartial. The person seeking disqualification bears the burden of proving otherwise. The trial

⁷*Burrows* was a revocation case, and the supreme court reversed and remanded for a new trial with a new judge because, prior to the revocation hearing, the sitting judge had requested that appellant bring his toothbrush and also made numerous other comments during the proceedings that created the appearance of partiality.

judge's decision not to recuse from a case is a discretionary one and will not be reversed on appeal absent an abuse of that discretion. An abuse of discretion can be shown by proving bias or prejudice on the part of the trial judge. To decide whether there has been an abuse of discretion, this court reviews the record to determine if prejudice or bias was exhibited. It is the appellant's burden to demonstrate such bias or prejudice.

(Citations omitted.)

We conclude that Walker failed to prove that the trial judge exhibited prejudice, and we hold that the trial judge's decision not to recuse himself was not an abuse of discretion. In *Carmical v. McAfee*, we stated that a trial judge is not required to recuse himself or herself if his or her former law partner is counsel in the proceeding at hand. 68 Ark. App. 313, 7 S.W.3d 350 (1999) (citing *Dolphin v. Wilson*, 328 Ark. 1, 942 S.W.2d 815 (1997)). Moreover, absent some objective demonstration by the appellant of the trial judge's prejudice, it is the communication of bias by the trial judge that will cause us to reverse his or her refusal to recuse. *Carmical, supra*. The mere fact that there were adverse rulings is not enough to demonstrate bias. *Id.* The fact that the trial judge and the prosecutor were former law partners did not require the trial judge's recusal, nor was there any demonstration of bias by the trial judge. Therefore, we reject Walker's argument that the trial judge was required to recuse from the case or that he abused his discretion in not recusing.

B. Suppression of Evidence

Walker next argues that the trial court erred in denying his motion to suppress the incriminating evidence based on his claim that the search of his apartment and computer equipment therein constituted a violation of his constitutional right against unreasonable

searches and seizures. Walker's narrow argument is that, although Microsoft and NCMEC (both private entities) had observed a hash value of a file that was catalogued as child pornography, neither of those private entities actually opened the file to view and confirm that the file image contained child pornography prior to providing the cyber tip to the Arkansas State Police. Walker argues that when Agent Pinner opened the file and viewed the image, he exceeded the scope of the private search and that the search warrant was invalid because it was based almost entirely on this illegally obtained information.

In reviewing the denial of a motion to suppress evidence, this court conducts a *de novo* review based on the totality of the circumstances, reviewing findings of historical facts for clear error and determining whether those facts give rise to reasonable suspicion or probable cause, giving due weight to inferences drawn by the trial court. *Lewis v. State*, 2023 Ark. 12. A finding is clearly erroneous, even if there is evidence to support it, when the appellate court, after review of the entire evidence, is left with the definite and firm conviction that a mistake has been made. *Id.* We defer to the superiority of the trial court to evaluate the credibility of witnesses who testify at a suppression hearing. *Id.*

In the affidavit for search warrant, Agent Pinner stated:

Microsoft OneDrive made the report to NCMEC on April 28, 2020. The cyber tip reported that one (1) image of apparent child pornography (unconfirmed) was uploaded to a Microsoft OneDrive Account. Microsoft OneDrive provided the image to NCMEC and I was eventually provided the image that was uploaded. The image is of a prepubescent minor male depicting nudity in a sexually suggestive pose.

Agent Pinner's affidavit went on to state that, with the IP address that had been provided in the cyber tip, it was later determined that the account associated with the IP address belonged

to Walker. Based on Agent Pinner's affidavit, a search warrant was issued, and the illicit images were found on Walker's computer during the search.

A hearing was held on Walker's motion to suppress. At the suppression hearing, both Agents Pinner and Battle testified about the investigation and the process by which hash values are instrumental in detecting and investigating child pornography.

Agent Pinner testified that he was assigned to investigate the cyber tip received from NCMEC. Pinner stated that he commonly works with such cyber tips in his investigative duties with the ICAC. Agent Pinner explained that the cyber tip was the result of hash-value identification from a known catalogue of images that had been previously determined to be child-sexual-abuse material. He compared a hash value to the DNA of a person. Agent Pinner stated that, although Microsoft and NCMEC had identified the file as containing known child pornography by the hash value and were in possession of the file before forwarding it to the Arkansas State Police, neither Microsoft employees nor NCMEC employees had actually viewed the image. Agent Pinner opened the file and confirmed its content as child pornography.

Agent Battle similarly testified that he is familiar with the cyber tipline used by NCMEC. Agent Battle stated that it is customary for him to receive cyber tips from NCMEC and, through those cyber tips, initiate an investigation and swear out an affidavit for a search warrant. Agent Battle stated that hash-value identification is instrumental in the cyber tips generated by NCMEC. Agent Battle explained that a hash value is a "digital fingerprint" of a file, which is unique to the file and the image it contains. Agent Battle stated that NCMEC

maintains a database of hash values that are known to contain child-sexual-abuse material. Thus, NCMEC is able to compare a known hash value to a file and, if the hash values match, determine that the file contains child pornography.

Both the United States and Arkansas Constitutions prohibit unreasonable searches and seizures not supported by probable cause or reasonable suspicion. U.S. Const. amend. IV; Ark. Const. art. II, § 15. Such limitations do not apply to searches conducted by private parties because, under the private-search doctrine, the prohibition against unreasonable searches and seizures does not apply to searches conducted by private citizens. *Whisenant v. State*, 85 Ark. App. 111, 146 S.W.3d 359 (2004). However, the government agency may not then exceed the scope of the private search unless it has the right to make an independent search. *Id.*

Walker argues that when law enforcement received a cyber tip from NCMEC regarding an unopened file that was alleged—but not visually confirmed—to contain child pornography, law enforcement exceeded the scope of the private search by opening the file. Walker argues that law enforcement lacked probable cause from the hash value itself, and that only by viewing the contents of the file did they have probable cause of criminal activity. When a search warrant is based on illegally obtained information, the appellate court examines the search warrant by excising the offending information from the search warrant and determines whether the affidavit nevertheless supports the issuance of a search warrant. *Lauderdale v. State*, 82 Ark. App. 474, 120 S.W.3d 106 (2003). Walker argues that, when excising from Agent Pinner’s affidavit his statement that the file image was of a prepubescent

minor male depicting nudity in a sexually suggestive pose, there was no probable cause to issue the search warrant. Walker thus argues that the trial court's denial of his motion to suppress was clearly erroneous. For the following reasons, we disagree.

In discussing the private-search doctrine in *Whisenant, supra*, we stated that there is no additional intrusion by the government agency during its inspection of the materials where the agent learned nothing that had not previously been learned during the private search. The critical inquiry is whether the authorities obtained information with respect to which the defendant's expectation of privacy had not already been frustrated. *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018). When the government's conduct merely confirms information gleaned in a private search and does not enable the government to discover information that had not previously been learned during the private search, it does not constitute a subsequent search. *United States v. Jacobsen*, 466 U.S. 109 (1984). In *Jacobsen*, the Supreme Court observed that protecting the risk of misdescription by the private party hardly enhances any legitimate privacy interest and is not protected by the Fourth Amendment.

Both Microsoft and NCMEC determined from the hash value of one of Walker's files that the file contained child pornography. Agents Pinner and Battle testified at the suppression hearing about hash-value technology and its accuracy and effectiveness in investigating internet crimes against children. Agent Pinner compared hash-value identification to a DNA match, and Agent Battle compared it to a fingerprint match. After both private entities observed the hash value and determined from the hash value that the

file contained child pornography, the information was forwarded to the Arkansas State Police. By opening the file and viewing its contents, Agent Pinner merely confirmed what had already been learned in the private search; therefore, no constitutional violation occurred.

In reaching our decision on the suppression issue, we are strongly persuaded by the Fifth Circuit Court of Appeals' decision in *Reddick, supra*. In *Reddick*, the defendant uploaded digital-image files to Microsoft SkyDrive. SkyDrive uses a program to automatically scan the hash values of user-uploaded files and compare them to the hash values of known images of child pornography. When a match is detected between the hash value of a user-uploaded file and a known child-pornography hash value, it creates a cyber tip and sends the file—along with the uploader's IP address information—to NCMEC. Microsoft sent cyber tips to NCMEC based on the hash values of files that the defendant had uploaded to SkyDrive. NCMEC then forwarded the cyber tip to the Corpus Christi Police Department. Upon receiving the cyber tip, a police officer opened the suspect files and confirmed that each contained child pornography. The police officer then applied for and received a warrant to search the defendant's home and seize his computer. The defendant argued that the police officer's warrantless opening of the files associated with the cyber tip—which were not first opened and viewed by Microsoft or NCMEC—was an unlawful search. The Fifth Circuit Court of Appeals disagreed.

Before addressing the merits of the suppression issue in *Reddick*, the federal appeals court set forth the following observations regarding hash-value technology and its usefulness in combating child pornography:

Private businesses and police investigators rely regularly on “hash values” to fight the online distribution of child pornography. Hash values are short, distinctive identifiers that enable computer users to quickly compare the contents of one file to another. They allow investigators to identify suspect material from enormous masses of online data, through the use of specialized software programs—and to do so rapidly and automatically, without the need for human searchers. Hash values have thus become a powerful tool for combating the online distribution of unlawful aberrant content.

....

In technical terms, a hash value is an “algorithmic calculation that yields an alphanumeric value for a file.” *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). More simply, a hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file’s contents. In the words of one commentator, “[t]he concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data.” Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005).

Hash values are regularly used to compare the contents of two files against each other. “If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output.” Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541 (2005). Hash values have been used to fight child pornography distribution by comparing the hash values of suspect files against a list of the hash values of known child pornography images currently in circulation. This process allows potential child pornography images to be identified rapidly, without the need to involve human investigators at every stage.

Reddick, 900 F.3d at 636–37.

The *Reddick* court concluded that the police officer did not conduct an illegal search when he viewed images that had not been actually viewed by Microsoft or NCMEC but had been identified by the private entities as child pornography by their hash values. The appeals court began by stating that, under the private-search doctrine, “the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant’s expectation of privacy had not already been frustrated.” *Reddick*, 900 F.3d at 638 (citing *United States v. Runyan*, 275 F.3d 449 (5th Cir. 2001)). The *Reddick* court stated that when the police officer first received the defendant’s files, he already knew their hash values matched the hash values of child-pornography images known to NCMEC. *Reddick*, 900 F.3d at 639. The court went on to state that hash-value comparison allows law enforcement to identify child pornography with almost absolute certainty because hash values are specific to the makeup of a particular image’s data, which can be described as a unique digital fingerprint. *Id.* The court held that when the police officer opened the files, there was no significant expansion of the search that had been conducted previously by a private party and that his visual review of the images merely dispelled any residual doubt about the contents of the files. *Id.* The federal appeals court in *Reddick* stated that the government effectively learned nothing from the police officer’s viewing of the files that it had not already learned from the private search, and that under the private-search doctrine, the government did not violate the defendant’s Fourth Amendment rights. *Id.* at 640.

We also find the Sixth Circuit Court of Appeals’ decision in *United States v. Miller*, 982 F.3d 412 (2020), to be instructive. In *Miller*, the appeals court also dealt with the issue

of whether a police officer could view images that had been identified by private entities as child pornography only by hash identification and not by visual inspection. The *Miller* court focused on the level of certainty of the hash identification. The court wrote:

The magistrate judge, whose findings the district court adopted, found that the technology was “highly reliable—akin to the reliability of DNA.” *United States v. Miller*, 2017 WL 9325815, at *10 (E.D. Ky. May 19, 2017). The evidence in one cited case suggested that “[t]he chance of two files coincidentally sharing the same hash value is 1 in 9,223,372,036,854,775,808.” *United States v. Dunning*, 2015 WL 13736169, at *2 (E.D. Ky. Oct. 1, 2015) (citation omitted). (That is 1 in 9.2 quintillion in case you were wondering.) Another cited source suggested that the common algorithms “will generate numerical identifiers so distinctive that the chance that any two data sets will have the same one, no matter how similar they appear, is less than one in one billion.” Barbara J. Rothstein et al., *Managing Discovery of Electronic Information: A Pocket Guide for Judges* 38 (2d ed. Federal Judicial Center 2012).

Miller, 982 F.3d at 430. The *Miller* court concluded that, through the information available, “a computer’s ‘virtual’ search of a single file creates more certainty about the file’s contents than a person’s ‘manual’ search of the file.” *Id.* The *Miller* court applied the private-search doctrine and rejected the defendant’s Fourth Amendment challenge. *Id.* at 431.⁸

The testimony by Agents Pinner and Battle at the suppression hearing showed that the hash-value match that resulted in the cyber tip from private entities was akin to a DNA match or fingerprint match. The reliability of hash-value matching to identify known child pornography was explained at length in both *Reddick* and *Miller*, discussed above. By visually

⁸We observe that Walker relies on the Ninth Circuit Court of Appeals decision in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), asserting that the appeals court in that case reached a different result than in *Reddick* or in *Miller* on similar facts. However, as stated, we are persuaded by the analysis in *Reddick* and *Miller*, and we apply those holdings to the facts herein.

inspecting the image provided by the private entities, Agent Pinner learned no more than had already been learned from the hash-value analysis of the private search, and his review of the image merely confirmed what was already known and dispelled any residual doubt about the contents of the file. *See Reddick, supra*. Therefore, we conclude that under the private-search doctrine, Agent Pinner's opening of the file did not violate Walker's constitutional right against unreasonable searches and seizures, and we hold that the trial court's denial of Walker's motion to suppress was not clearly erroneous.

C. Admission of Prior Crimes

Walker's next argument is that the trial court erred by admitting Walker's prior convictions during the guilt phase of the trial. Prior to trial, the State filed a notice of intent to introduce evidence pursuant to Rule 404(b) of the Arkansas Rules of Evidence. This evidence consisted of Walker's three 2009 Oregon convictions for encouraging child sexual abuse in the first degree. Walker subsequently filed a motion in limine to exclude the convictions, arguing that they were inadmissible under Rule 404(b) and also that the evidence was more prejudicial than probative under Rule 403. After a hearing on Walker's motion in limine, the trial court denied the motion and allowed the State to introduce the convictions at trial.

Rule 404(b) provides:

Other Crimes, Wrongs, or Acts. Evidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show that he acted in conformity therewith. It may, however, be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident.

The State is not entitled to introduce evidence of other offenses to persuade the jury that the accused is a criminal and likely to commit the crimes he has been charged with. *Green v. State*, 365 Ark. 478, 231 S.W.3d 638 (2006). However, if the evidence of another crime, wrong, or act is relevant to show that the offense of which appellant is accused actually occurred and is not introduced merely to prove bad character, it will not be excluded. *Lindsey v. State*, 319 Ark. 132, 890 S.W.2d 584 (1994). In dealing with issues relating to the admission of evidence pursuant to Rule 404(b), a trial court's ruling is entitled to great weight, and this court will not reverse absent an abuse of discretion. *Green, supra*.

Walker argues that the trial court abused its discretion in admitting the prior convictions under Rule 404(b) because this evidence was not independently relevant to prove some material point at issue but was rather introduced merely to prove he is a criminal. We disagree.

The statutory elements of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child—with which Walker was charged in this case—are very similar to the elements of encouraging child sexual abuse in the first degree under the 2009 version of the Oregon statute upon which Walker was convicted.⁹ Moreover, the record reveals factual similarities between Walker's Oregon convictions and the charges herein. Here, the proof showed that Walker possessed multiple images on his computer of

⁹At the time of Walker's 2009 Oregon convictions, the elements of Or. Rev. Stat. § 163.684 prohibited possessing photographs or other visual recordings of sexually explicit conduct involving a child.

juvenile males in sexually explicit poses and juvenile males engaged in sexually explicit conduct with adult males. In the Oregon case, the investigation began when a public library reported that a printed copy of an adult male sodomizing a juvenile was discovered in a restroom. The police confirmed that Walker's fingerprints were on the photograph, and a subsequent search of a flash drive in Walker's possession uncovered 120 images of nude juveniles, juveniles in sexually explicit poses, and a juvenile engaging in sexual acts. Walker admitted to the Oregon authorities that he had downloaded these images from a computer.

We conclude that the Oregon convictions were probative of Walker's knowledge and intent under Rule 404(b). Walker's defense at trial was that he simply did not possess any of the illegal images attributed to him, as he stated in his opening argument and argued in his directed-verdict motion and closing argument. In Walker's custodial interview with the police, Walker denied possessing child pornography on his computer equipment. Therefore, the prior convictions for similar conduct were relevant to establish Walker's knowledge and intent to commit these crimes. The supreme court has held that Rule 404(b) evidence is admissible to prove knowledge and intent of the criminal defendant due to similar conduct. *See, e.g., Davis v. State*, 362 Ark. 34, 207 S.W.3d 474 (2005) (similar incident of sexual assault admitted to show intent); *Fells v. State*, 362 Ark. 77, 207 S.W.3d 498 (2005) (victim of similar, but earlier, rape by defendant allowed to prove intent, motive, or plan); *see also Nelson v. State*, 365 Ark. 314, 229 S.W.3d (2006) (affirming the admission of multiple prior drug convictions to show intent when Nelson claimed he was simply in the car and the drugs

found there belonged to another passenger.) For these reasons, we hold that the trial court's decision to admit the prior convictions under Rule 404(b) was not an abuse of discretion.

However, as Walker points out in his brief, even if evidence is relevant under Rule 404(b), Arkansas Rule of Evidence 403 provides that evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice. The standard of review for the admission of Rule 403 evidence is whether the trial court abused its discretion. *Harmon v. State*, 286 Ark. 184, 690 S.W.2d 125 (1985). Walker argues that, even if the evidence of his prior convictions had some probative value, the evidence was unfairly prejudicial under Rule 403. We, however, disagree with this argument as well. In *Rounsaville v. State*, 374 Ark. 356, 288 S.W.3d 213 (2008), the supreme court stated that evidence offered by the State in a criminal trial is likely to be prejudicial to the defendant to some degree, otherwise it would not be offered. On this record, we find no abuse of discretion in the trial court's determination that the probative value of Walker's prior convictions was not substantially outweighed by the danger of unfair prejudice. Therefore, we find no error in the admission of the prior crimes.

D. Admission of Uncharged Images

In Walker's pretrial motion in limine, he also argued that the State should be prohibited from introducing other images seized from his computer for which he was not charged. After the hearing on Walker's motion, the trial court denied that portion of Walker's motion and ruled that these other images were admissible, and Walker now asserts that this was erroneous.

During Agent Battle's trial testimony, he explained that child-sexual-abuse material is the same thing as child pornography. Agent Battle testified that State's exhibits 1-30 contained images of child-sexual-abuse material, and these exhibits were admitted as evidence of Walker's guilt on the charged offenses. Agent Battle explained further that child-exploitative material is material depicting a child that may be in a provocative or sexual pose, but the child is clothed. Over Walker's objection, the State was permitted to admit exhibits 31-45, for which Walker was not charged and that consisted of fifteen images from Walker's computer containing child-exploitative material.

Walker argues that the introduction of these uncharged images violated Rule 404(b) because they served no legitimate purpose and were introduced only to show his propensity for viewing child-exploitative material. Walker also argues that this evidence was inadmissible because it was extremely prejudicial.

The mere fact that a photograph is inflammatory or is cumulative is not, standing alone, sufficient reason to exclude it. *Lewis v. State*, 2023 Ark. 12. However, if a photograph serves no valid purpose and could be used only to inflame the jurors' passions, it should be excluded. *Id.*

The State argues that the images of child-exploitative material were relevant to show Walker's predilection for sexualized images of prepubescent boys and to show knowledge, intent, absence of mistake, or accident under Rule 404(b), and we agree. In *Lewis, supra*, the supreme court affirmed the admission of additional uncharged pornographic images, stating that "[g]iven Lewis's defense that he lacked knowledge, the admission of the additional

images was relevant to show knowledge, intent, and absence of mistake or accident.” *Lewis*, 2023 Ark. 12, at 19–20; *see also Steele v. State*, 2014 Ark. App. 257 (holding that evidence of computer images of child pornography, for which Steele was not charged with possessing, was relevant to show knowledge, intent, and absence of mistake and was thus properly admitted in prosecution for distributing, possessing, or viewing child pornography on his computer). Moreover, the fifteen additional images introduced in this case that contained child-exploitative material were not unfairly prejudicial because they were less inflammatory than the thirty images depicting child-sexual-abuse material that had already been introduced and for which Walker was being charged. For these reasons, we hold that the trial court did not abuse its discretion in admitting the uncharged images at trial.

E. Admission of Walker’s Statement to the Police
Pertaining to Sex-Offender Registration

Walker next argues that the trial court erred in allowing the State to play the portion of his custodial statement to the police where the officer incorrectly alleged that Walker was delinquent in his sex-offender registration. Walker again cites Rule 404(b) and argues a violation of that evidentiary rule and further argues that any probative value of this evidence was substantially outweighed by the danger of unfair prejudice.

During the search of Walker’s apartment, Walker gave a Mirandized statement to Agent Pinner. Prior to the introduction of the recording of the statement at trial, Walker objected to the portions in which his sex-offender status was discussed, and the trial court overruled the objection. In the custodial interview that was played to the jury, Agent Pinner

asked whether Walker had ever been arrested for child pornography, and Walker replied no. Agent Pinner then asked whether Walker was a registered sex offender and whether he had failed to register in Arkansas, and Walker replied no to both questions. Later in the interview, Agent Pinner again questioned whether Walker was a sex offender in Oregon and whether he was delinquent there, and Walker denied that accusation, indicating that he was current on his Oregon sex-offender registration. Agent Pinner then suggested that “your problem right now” is that “you have not registered in the state of Arkansas.” Walker replied, “Okay.”

We conclude that any error in admitting the discussion pertaining to Walker’s sex-offender status was harmless. We may declare an evidentiary error harmless if the evidence of guilt is overwhelming and the error is slight. *Johnston v. State*, 2014 Ark. 110, 431 S.W.3d 895. As we have already explained, the trial court committed no error in admitting Walker’s three prior Oregon convictions for encouraging child sexual abuse in the first degree, so the jury knew about Walker’s sex-offender status from competent evidence independent of the police interview. Moreover, any possible error with respect to whether Walker had registered as a sex offender in this state was slight when compared to the overwhelming evidence of his guilt for the crimes charged. Therefore, no reversible error occurred under this point.

F. Admission of Walker’s Oregon Pen Pack

Walker next argues that the trial court erred in admitting his Oregon “pen pack” during the guilt phase of the trial. Walker argues that any marginal probative value of the contents of the pen pack was grossly outweighed by the danger of unfair prejudice and

confusing the issues. In particular, Walker points out that his pen pack contained a reference to a drug-possession case, information that he was indigent, and information about his mandatory mental-health treatment for sexually deviant behavior.

We conclude that this argument is not preserved for review. When the State introduced evidence of Walker's convictions at trial (which had already been ruled admissible prior to trial) it stated, "[I]t is in the form of a pen pack." Walker objected, arguing:

With regard to this, the court did make a decision that it could be admissible. Our objection would be to the way it's being admitted at this point in time Whether or not the document could come in is not an issue, but how it comes in I believe the keeper of the records would have to be here for this to be introduced.

At trial, Walker's only objection to the pen pack was, in effect, for lack of foundation and that it should not be admitted without the record keeper to introduce it. Walker does not make that argument on appeal; rather, his argument on appeal is that the specific information in the pen pack was unduly prejudicial. Our law is well established that in order to preserve a challenge for our review, the movant must apprise the trial court of the specific basis on which the motion is made. *Stewart v. State*, 320 Ark. 75, 894 S.W.2d 930 (1995). Parties may not change their arguments on appeal and are limited to the scope and nature of their arguments made below. *Id.* Because Walker has changed his argument on appeal, we will not address it.

G. Affirmative-Defense Jury Instruction

Walker next argues that the trial court erred in denying his request for an affirmative-defense jury instruction based on Ark. Code Ann. § 5-27-602(c), which provides, “It is an affirmative defense to a prosecution under this section that the defendant in good faith reasonably believed that the person depicted in the matter was seventeen (17) years of age or older.” Walker requested this jury instruction with respect to only five of the thirty images for which he was charged. Walker argues that the jury instruction should have been given with respect to those five charges because, at the very least, those images contained the slightest evidence that they could involve persons seventeen years of age or older.

A party is entitled to a jury instruction when it is a correct statement of the law and when there is some basis in the evidence to support giving the instruction. *Vidos v. State*, 367 Ark. 296, 239 S.W.3d 467 (2006). We will not reverse a trial court’s decision to give an instruction unless the court abused its discretion. *Id.*

We hold that the trial court did not abuse its discretion in denying the affirmative-defense jury instruction. Walker’s defense at trial was that he did not possess any of the illegal images attributed to him, as he stated in his opening argument and argued in his directed-verdict motion and closing argument. In Walker’s custodial interview with the police, Walker denied possessing child pornography on his computer equipment. From the evidence presented, there was no basis in the evidence to conclude that Walker reasonably believed that some of the images found on his computer depicted persons seventeen years of age or older. Therefore, this argument is without merit.

H. Illegal Sentence – Sexually Dangerous Person

Finally, in his reply brief, Walker raises an issue that a portion of his sentence was illegal. Normally, an appellant may not raise an issue for the first time in his reply brief. See *Adams v. State*, 2020 Ark. App. 501, 612 S.W.3d 191. However, we may address an illegal sentence sua sponte, *Muhammad v. State*, 2021 Ark. 129, 624 S.W.3d 300, and when an error has nothing to do with the issue of guilt or innocence and relates only to punishment, it may be corrected in lieu of reversing and remanding. *Bangs v. State*, 310 Ark. 235, 835 S.W.2d 294 (1992). For the following reasons, we conclude that a portion of Walker’s sentence was illegal.

In the sentencing order, the trial court checked the yes box for: “Defendant is alleged to be a sexually dangerous person and is ordered to undergo an evaluation at a facility designated by A.D.C. pursuant to A.C.A. § 12-12-918.” However, this designation in the sentencing order was erroneous. Arkansas Code Annotated section 12-12-918 (Supp. 2021 2021) provides, in relevant part:

(a)(1) In order to classify a person as a sexually dangerous person, a prosecutor may allege *on the face of an information* that the prosecutor is seeking a determination that the defendant is a sexually dangerous person.

(2)(A) If the defendant is adjudicated guilty, the court shall enter an order directing an examiner qualified by the Sex Offender Assessment Committee to issue a report to the sentencing court that recommends whether or not the defendant should be classified as a sexually dangerous person.

(Emphasis added.) Here, the State did not allege on the face of the original information or on the face of the amended information that it was seeking a determination that Walker is

a sexually dangerous person. Therefore, we modify and correct the sentencing order to delete this designation.

III. *Conclusion*

In conclusion, we find merit in none of Walker's arguments on appeal, and we affirm his convictions for thirty counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child. However, we modify the sentencing order as explained above.

Affirmed as modified.

MURPHY and BROWN, JJ., agree.

Lassiter Cassinelli, by: *Michael Kiel Kaiser*, for appellant.

Leslie Rutledge, Att'y Gen., by: *Joseph Karl Luebke*, Ass't Att'y Gen., and *Karen Virginia Wallace*, Ass't Att'y Gen., for appellee.